Background

These attacks are pretty much the same as in any cloud. If the compromised user is assigned the role "Global Reader" or "Global Contributor" you might be able to read some sensitive data.

- You try to read keyvault.
- Application Service configurations - might contain creds - deplyment credentisl, database credentials.
- Automation accounts - Credentials for azure automation accounts

Just like any privilege escalation attack in a cloud provider.

Pre-requisites

Access to an Azure account which is associated with an azure subscription.

```
# Login using azure cli
az login

# list subscriptions
az account list
```

If no subscriptions are associated with the user you won't be able to do much.

Your user must have the role `Global Reader` assigned to it.

Risks

No risks.

How to check for

https://github.com/hausec/PowerZure PowerZure can be used to check for secrets.

```
get-runbooks
```

How to exploit

Recommendation

Related Vulnerabilities

References

https://www.youtube.com/watch?v=AWhag2K3AS8